CLAIMS

What is claimed is:

1. A method for computing a group shared secret key at a first node of a network for use in a public key process and using less than n * (n-1) messages, where "n" is a number of nodes in a broadcast or multicast group of the network, the method comprising the computer-implemented steps of:

generating an intermediate shared secret key by issuing communications to a second node of the network;

sending a first private value associated with the first node to the second node, and receiving from the second node a second private value associated with the second node using the intermediate shared secret key;

generating and communicating a collective public key that is based upon the first private value and the second private value to a third node of the network;

receiving an individual public key from the third node; and

computing and storing the group shared secret key based upon the individual public key.

2. The method as recited in Claim 1, further comprising:

joining the first node to an initial multicast group in response to generating the intermediate shared secret key; and

joining a second node to a new multicast group that subsumes the initial multicast group after receiving the individual public key.

3. The method as recited in Claim 1, wherein the public-key process is Diffie-Hellman key exchange.

4. The method as recited in Claim 1, wherein the step of communicating the collective public key further comprises determining whether the first node or the second node transfers the collective public key based upon an order of entry of such nodes into a multicast group.

5. The method as recited in Claim 1, wherein the step of communicating the collective public key further comprises determining whether the first node or the second node transfers the collective public key based upon a predetermined metric.

6. The method as recited in Claim 1, wherein sending the first private value and receiving the second private value further comprises computing the first private value as a random integer and receiving a second random integer as the second private value.

7. The method as recited in Claim 1, further comprising creating and storing information at the first node that associates the first node, the second node, and the third node as a multicast group communicating over a packet switched network.

8. The method as recited in Claim 1, wherein the steps of generating, sending, communicating, and receiving further comprise communicating approximately 2n + 2(n-1) total messages.

9. The method as recited in Claim 1, wherein the step of communicating the collective public key comprises storing the collective public key and receiving the collective public key using a key distribution center.

10. The method as recited in Claim 1, further comprising the step of establishing a cryptographic communication session between the first node and the second node, whereby secure communications are established between the first and the second node using public key exchange and only approximately 2n + 2(n-1) total messages.

11. A method as recited in Claim 1, wherein generating the shared secret key value comprises computing and storing the shared secret key value "k" at the first node according to the relation

$$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$$

wherein C, a, b, c, q, and p are values stored in a memory, and wherein C is the individual public key, a is the private value of the first node, b is the private

value of the second node, c is a third private value of the third node, p is a base value, and q is a prime number value.

12. A method for exchanging cryptographic keys among a plurality of nodes in a multicast or broadcast group, the method comprising the computer-implemented steps of:

(a) computing and storing a first shared secret key at a first node;

(b) transmitting a first message, encrypted using the first shared secret key, to a second node;

(c) receiving a second message, encrypted using the first shared secret key, from the second node;

(d) computing and storing a first public key based upon the first and second messages;

(e) transmitting the first public key to a third node;

(f) receiving a second public key from the third node;

(g) computing a second shared secret key based upon the second public key, the first message, and the second message;

(h) iteratively performing steps of (e) through (g) until the nodes reach a group shared secret key for use in cryptographic communication among the of nodes, and using less than n * (n-1) total messages;

whereby the first node and second node independently come to a shared secret key value.

13. The method as recited in Claim 12, further comprising:

joining the first node to an initial multicast group in response to generating the first public key; and

joining the first node to a new multicast group that subsumes the initial multicast group after receiving the second public key.

14. The method as recited in Claim 12, wherein the step of transmitting the first public key further comprises determining whether the first node or the second node transfers the first public key based upon an order of entry of such nodes into a multicast group.

15. The method as recited in Claim 12, further comprising creating and storing information at the first node that associates the first node, the second node, and the third node as a multicast group communicating over a packet switched network.

16. The method as recited in Claim 12, wherein step (h) comprises the step of:

(h) iteratively performing steps of (e) through (g) until the nodes reach a group shared secret key for use in cryptographic communication among the of nodes, and using approximately $2n + 2(n-1)$ total messages.

17. The method as recited in Claim 12, further comprising communicating with a key distribution center to obtain public keys for use in arriving at a shared secret value.

18. The method as recited in Claim 12, further comprising the step of establishing a cryptographic communication session between the nodes, whereby secure communications are established between the nodes using public key exchange and only approximately $2n + 2(n-1)$ total messages.

19. A method as recited in Claim 12, wherein generating the shared secret key value comprises computing and storing the first shared secret key value "k" at the first node according to the relation

$$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$$

wherein C, a, b, c, q, and p are values stored in a memory, and wherein C is the individual public key, a is the private value of the first node, b is the private value of the second node, c is a third private value of the third node, p is a base value, and q is a prime number value.

20. A computer-readable medium carrying one or more sequences of one or more instructions for computing a group shared secret key at a first node of a network for use in a public key process and using less than n * (n-1) messages, where "n" is a number of nodes in a broadcast or multicast group of the network, and which instructions, when executed by one or more processors, cause the one or more processors to perform the steps of:

generating an intermediate shared secret key by issuing communications to a second node of the network;

sending a first private value associated with the first node to the second node, and receiving from the second node a second private value associated with the second node using the intermediate shared secret key;

generating and communicating a collective public key that is based upon the first private value and the second private value to a third node of the network;

receiving an individual public key from the third node; and

computing and storing the group shared secret key based upon the individual public key.

21. The computer-readable medium recited in Claim 20, wherein the instructions further cause the one or more processors to carry out the steps of:

joining the first node to an initial multicast group in response to generating the intermediate shared secret key; and

joining the first node to a new multicast group that subsumes the initial multicast group after receiving the individual public key.

22. The computer-readable medium as recited in Claim 20, wherein the public-key process is Diffie-Hellman key exchange.

23. The computer-readable medium as recited in Claim 20, wherein the instructions for communicating the collective public key further comprise instructions for determining whether the first node or the second node transfers the collective public key based upon an order of entry of such nodes into a multicast group.

24. The computer-readable medium as recited in Claim 20, wherein the instructions for communicating the collective public key further comprise instructions for determining whether the first node or the second node transfers the collective public key based upon a predetermined metric.

25. The computer-readable medium as recited in Claim 20, wherein the instructions for sending the first private value and receiving the second private value further comprise instructions for computing the first private value as a random integer and receiving a second random integer as the second private value.

26. The computer-readable medium as recited in Claim 20, further comprising instructions for creating and storing information at the first node that associates the first node, the second node, and the third node as a multicast group communicating over a packet switched network.

27. The computer-readable medium as recited in Claim 20, wherein the instructions for generating, sending, communicating, and receiving further comprise instructions that communicate only approximately $2n + 2(n-1)$ total messages.

28. The computer-readable medium as recited in Claim 20, wherein the instructions for communicating the collective public key further comprise instructions for storing the collective public key and receiving the collective public key using a key distribution center.

29. The computer-readable medium as recited in Claim 20, further comprising instructions for establishing a cryptographic communication session between the first node and the second node, whereby secure communications are established between the first and the second node using public key exchange and only approximately $2n + 2(n-1)$ total messages.

30. A computer-readable medium as recited in Claim 20, wherein the instructions for generating the shared secret key value further comprise instructions for computing and storing the shared secret key value "k" at the first node according to the relation

$$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$$

wherein C, a, b, c, q, and p are values stored in a memory, and wherein C is the individual public key, a is the private value of the first node, b is the private value of the second node, c is a third private value of the third node, p is a base value, and q is a prime number value.